

**BURSOR & FISHER, P.A.**

L. Timothy Fisher (State Bar No. 191626)

1990 North California Blvd., Suite 940

Walnut Creek, CA 94596

Telephone: (925) 300-4455

Facsimile: (925) 407-2700

Email: ltfisher@bursor.com

*Counsel for Plaintiff*

**UNITED STATES DISTRICT COURT**

**NORTHERN DISTRICT OF CALIFORNIA**

M.D., individually and on behalf of all others  
similarly situated,

Plaintiff,

v.

GOOGLE LLC and META PLATFORMS,  
INC.,

Defendants.

Case No.

**CLASS ACTION COMPLAINT**

**JURY TRIAL DEMANDED**

Plaintiff M.D. (“Plaintiff”) brings this class action complaint on behalf of himself and all others similarly situated (the “Class Members”) against Defendants Google LLC (“Google”) and Meta Platforms, Inc. (“Facebook”)<sup>1</sup> (together with Google, “Defendants”). Plaintiff brings this action based on personal knowledge of the facts pertaining to himself, and on information and belief as to all other matters, by and through the investigation of undersigned counsel.

### **NATURE OF THE ACTION**

1. This is a class action brought on behalf of all patients who accessed and used [www.bluechew.com](http://www.bluechew.com) (the “Website”) to purchase prescription medication.

2. Dermacare, LLC d/b/a BlueChew (hereinafter, “BlueChew”) provides “a technology platform which enables registered users to connect with physicians and other health care providers for the diagnosis and treatment of erectile dysfunction.”<sup>2</sup> The Website offers patients convenient and discrete access to prescription medications for the treatment of this medical condition.

3. Information concerning an individual’s healthcare and prescription medication is protected by state and federal law. Despite these protections, and unbeknownst to Plaintiff and Class Members, this sensitive, personal information communicated through the Website was intercepted by some of the largest advertising and social media companies in the country, including Facebook and Google.

4. Defendants intercepted this protected information through tracking technology embedded on the Website, including software development kits (“SDK”) and tracking pixels.

5. The protected information intercepted by Defendants was not aggregated or deidentified nor were Defendants prohibited from using this information for their own benefit. Defendants used this information for their own purposes, including for targeted advertising.

6. Plaintiff and Class Members provided their personal information, including prescription information, to BlueChew with the expectation that this information would remain confidential and private. Defendants’ interception of this information without explicit consent

<sup>1</sup> In October 2021, Facebook, Inc. changed its name to Meta Platforms, Inc. Unless otherwise indicated, Facebook, Inc. and Meta Platforms, Inc. are referenced collectively as “Facebook.”

<sup>2</sup> BlueChew, Terms and Conditions, <https://bluechew.com/terms-and-conditions>.

1 constitutes an extreme invasion of Plaintiff's and Class Members' privacy. Plaintiff brings this  
2 action for legal and equitable remedies resulting from these illegal actions.

3 **PARTIES**

4 7. Plaintiff M.D. is a California citizen who resides in Whittier, California. On  
5 December 6, 2022, and January 4, 2023, Plaintiff was prescribed and ordered Sildenafil erectile  
6 dysfunction medication through the Website. Unbeknownst to Plaintiff, Google and Facebook  
7 intercepted protected health information ("PHI") related to his prescription medication through  
8 their proprietary software codes, as described more thoroughly below. Due to the surreptitious  
9 nature of the interceptions at issue, Plaintiff did not realize confidential information related to his  
10 medical prescription was disclosed to third parties until September 2024. Plaintiff was in  
11 California when he ordered prescription medication through the Website.

12 8. In addition to information related to his prescription medication, Defendants also  
13 intercepted Plaintiff's personally identifiable information ("PII"), including his first and last name,  
14 email address, and date of birth. Subsequently, as a result of Defendants' conduct, Plaintiff has  
15 received targeted advertisements relating to erectile dysfunction medications.

16 9. Facebook and Google committed the interceptions at issue without Plaintiff's  
17 knowledge, consent, or express written authorization. Such acts are egregious violations of  
18 Plaintiff's right to privacy.

19 10. Defendant Google LLC is a Delaware limited liability company with its principal  
20 place of business located in Mountain View, California. At all times, Defendant Google knew that  
21 the incorporation of its software onto the Website would result in its interception of PHI and other  
22 sensitive data from the Website. Defendant Google, as the creator of its SDK, knew that it  
23 intercepted each of a users' interactions on the Website that incorporated its technology.  
24 Defendant Google has consistently come under scrutiny for incorporating its technology on  
25 websites that involve the transmittal of sensitive data, including health information, but continues  
26 to do so. Despite this, Google took no action to prevent its tracking technology from being  
27 embedded on the Website, from which it intercepted BlueChew patients' sensitive health data.  
28

11. Defendant Meta Platforms, Inc. is a Delaware corporation with its principal place of business located in Menlo Park, California. Defendant Facebook at all times knew that the incorporation of its software onto the Website would result in its interception of PHI and other sensitive data from the Website. Defendant Facebook, as the creator of its software, known as the Facebook Tracking Pixel, knew that it intercepted each of a users' interactions on the Website that incorporated its technology. Defendant Facebook has consistently come under scrutiny for incorporating its technology on websites that involve the transmittal of sensitive data, including health information, but continues to do so. Facebook's own employees have confirmed that Facebook lacks the ability to prevent the collection of sensitive health data or its use in ads. For example, Facebook engineers on the ad and business product team wrote in a 2021 privacy review "[w]e do not have an adequate level of control and explainability over how our systems use data, and thus we can't confidently make controlled policy changes or external commitments such as 'we will not use X data for Y purpose.'" As demonstrated by the continued incorporation of the Facebook Tracking Pixel on the Website, Facebook did not take any steps to prevent its interception and use of BlueChew patients' sensitive health data.

#### **JURISDICTION AND VENUE**

12. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because at least one member of the Class, as defined below, is a citizen of a different state than the Defendants, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds \$5,000,000.00 exclusive of interest and costs.

13. This Court has personal jurisdiction over the parties because the parties reside in California, are California citizens, and submit to the jurisdiction of the Court. Further, Defendants have, at all times relevant hereto, resided in this District.

14. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendants transact significant business within this District and Defendants reside in this District.

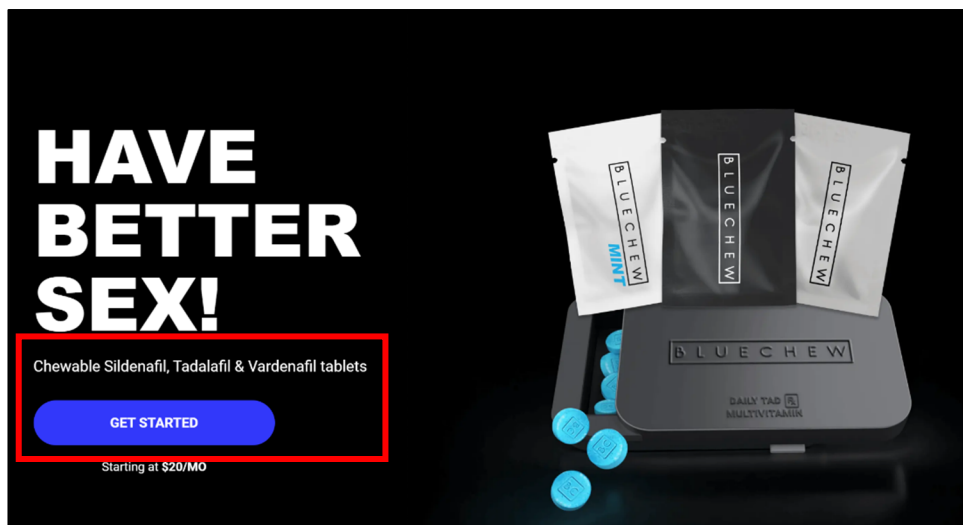
## FACTUAL ALLEGATIONS

### **A. The BlueChew Website**

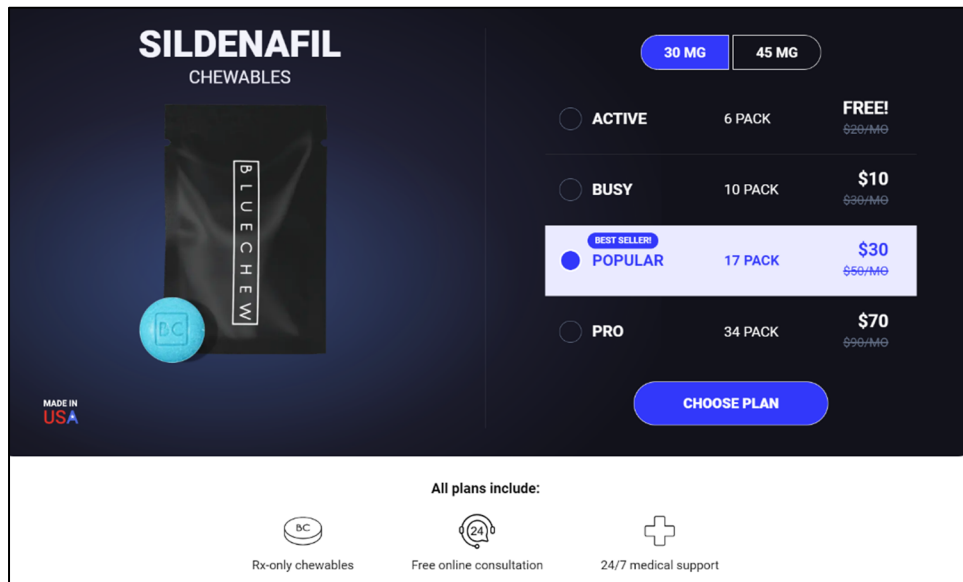
15. BlueChew is a telemedicine platform that was founded in 2014. BlueChew offers its patients three different forms of erectile dysfunction prescription medications. The three prescriptions offered by BlueChew contain the same active ingredients as popular brand name erectile dysfunction medications, such as Viagra (Sildenafil), Cialis (Tadalafil), and Levitra (Vardenafil).

16. Consumers can only order prescription medication from BlueChew through its Website. When patients visit the Website, they are brought to BlueChew's homepage to order a prescription.

**Figure 1:**



17. Once a consumer clicks “GET STARTED,” they are brought to an additional page to select a prescription plan.

**Figure 2:**

18. After selecting a prescription plan, patients are directed to complete a “medical profile” questionnaire, to determine whether they qualify for their selected prescription.

**Figure 3:**

The screenshot shows the 'MEDICAL PROFILE' section of a website. It begins with the heading 'MEDICAL PROFILE' and a sub-heading 'Please answer the following questions to get your order approved.' Below this, there is a section titled '1. Enter your personal information.' which contains three input fields: 'Legal First Name (as it appears on ID)', 'Legal Last Name (as it appears on ID)', and 'Birth Date (MM/DD/YYYY)'.

19. When completing their medical profile on the Website, consumers are asked a range of health-related questions and asked to provide basic PII, including first and last name and date of birth.

20. If a patient is approved for their selected prescription medication, they are brought to a checkout page to complete their purchase.

**Figure 4:**

The screenshot shows a checkout page for BlueChew. On the left, there is a 'Shipping Address' form with fields for Legal First Name\*, Legal Last Name\*, Street Address\*, Apt, suite, etc. (Optional), City\*, State\*, Zip Code\*, and Phone\*. Below the form is a blue button labeled 'Add Shipping Address'. On the right, there is a product image of a box of Sildenafil Chewables (BlueChew) and a summary of the order. The summary includes the product name 'SILDENAFIL Chewables', the quantity 'POPULAR 17 PACK | 30 MG (\$50/MO)', a coupon code 'GET20', and a price breakdown: Price (\$50.00 /MO), Shipping (TBD), Coupon (- \$20.00), Handling Fee & Tax (TBD), and a Grand Total of \$30.00.

21. At no point during the checkout process are patients alerted that information related to their prescription medication is being intercepted by third parties.

#### **B. Facebook's Tracking Technology on the BlueChew Website**

22. Facebook describes itself as a “real identity platform,”<sup>3</sup> meaning users are allowed only one account and must share “the name they go by in everyday life.”<sup>4</sup> To that end, when creating an account, users must provide their first and last name, along with their birthday and gender.<sup>5</sup>

23. In 2023, Facebook generated over \$134 billion in revenue.<sup>6</sup> With respect to the apps offered by Facebook, substantially all of Facebook's revenue is generated by selling advertising space.<sup>7</sup>

<sup>3</sup> Sam Schechner & Jeff Horwitz, *How Many Users Does Facebook Have? The Company Struggles to Figure It Out*, WALL ST. J. (Oct. 21, 2021, 4:05 PM), <https://www.wsj.com/articles/how-many-users-does-facebook-have-the-company-struggles-to-figure-it-out-11634846701>.

<sup>4</sup> FACEBOOK, COMMUNITY STANDARDS, PART IV INTEGRITY AND AUTHENTICITY, [https://www.facebook.com/communitystandards/integrity\\_authenticity](https://www.facebook.com/communitystandards/integrity_authenticity).

<sup>5</sup> FACEBOOK, SIGN UP, <https://www.facebook.com>.

<sup>6</sup> FACEBOOK, META REPORTS FOURTH QUARTER AND FULL YEAR 2023 RESULTS; INITIATES QUARTERLY DIVIDEND, [https://s21.q4cdn.com/399680738/files/doc\\_news/Meta-Reports-Fourth-Quarter-and-Full-Year-2023-Results-Initiates-Quarterly-Dividend-2024.pdf](https://s21.q4cdn.com/399680738/files/doc_news/Meta-Reports-Fourth-Quarter-and-Full-Year-2023-Results-Initiates-Quarterly-Dividend-2024.pdf) at 8.

<sup>7</sup> *Id.*

24. Facebook sells advertising space by highlighting its ability to target users.<sup>8</sup> Facebook can target users effectively because it surveils user activity on and off its site.<sup>9</sup> This allows Facebook to make inferences about users beyond what they explicitly disclose, like their “interests,” “behavior,” and “connections.”<sup>10</sup> Facebook compiles this information into a generalized dataset called “Core Audiences,” which allows advertisers to reach precise audiences based on specified targeting types.<sup>11</sup>

25. Advertisers can also build “Custom Audiences.”<sup>12</sup> Custom Audiences enables advertisers to reach “people who have already shown interest in [their] business, whether they’re loyal customers or people who have used [their] app or visited [their] website.”<sup>13</sup> With Custom Audiences, advertisers can target existing customers directly and build “Lookalike Audiences,” which “leverage[] information such as demographics, interests and behaviors from your source audience to find new people who share similar qualities.”<sup>14</sup> Unlike Core Audiences, advertisers can build Custom Audiences and Lookalike Audiences only if they first supply Facebook with the underlying data. They can do so through two mechanisms: (1) by manually uploading contact information for customers or (2) by utilizing Facebook’s “Business Tools.”<sup>15</sup>

26. As Facebook puts it, the Business Tools “help website owners and publishers, app developers, and business partners, including advertisers and others, integrate with [Facebook],

<sup>8</sup> FACEBOOK, WHY ADVERTISE ON FACEBOOK, INSTAGRAM AND OTHER META TECHNOLOGIES, <https://www.facebook.com/business/help/205029060038706>.

<sup>9</sup> FACEBOOK, ABOUT META PIXEL, <https://www.facebook.com/business/help/742478679120153?id=1205376682832142>.

<sup>10</sup> FACEBOOK, AD TARGETING: HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, <https://www.facebook.com/business/ads/ad-targeting>.

<sup>11</sup> FACEBOOK, <https://www.facebook.com/business/news/Core-Audiences>.

<sup>12</sup> FACEBOOK, ABOUT CUSTOM AUDIENCES, <https://www.facebook.com/business/help/744354708981227?id=2469097953376494>.

<sup>13</sup> FACEBOOK, AUDIENCE AD TARGETING, <https://www.facebook.com/business/ads/ad-targeting>.

<sup>14</sup> FACEBOOK, ABOUT LOOKALIKE AUDIENCES, <https://www.facebook.com/business/help/164749007013531?id=401668390442328>.

<sup>15</sup> FACEBOOK, CREATE A CUSTOMER LIST CUSTOM AUDIENCE, <https://www.facebook.com/business/help/170456843145568?id=2469097953376494>; FACEBOOK, CREATE A WEBSITE CUSTOM AUDIENCE, <https://www.facebook.com/business/help/1474662202748341?id=2469097953376494>.

1 understand and measure their products and services, and better reach and serve people who might  
 2 be interested in their products and services.”<sup>16</sup> Put more succinctly, Facebook’s Business Tools are  
 3 bits of code that advertisers can integrate into their websites, mobile applications, and servers,  
 4 thereby enabling Facebook to intercept and collect user activity on those platforms.

5 27. The Business Tools are automatically configured to capture certain data, like when a  
 6 user visits a webpage, that webpage’s Universal Resource Locator (“URL”) and metadata, or when  
 7 a user downloads a mobile application or makes a purchase.<sup>17</sup> Facebook’s Business Tools can also  
 8 track other events. Facebook offers a menu of “standard events” from which advertisers can  
 9 choose, including what content a visitor views or purchases.<sup>18</sup> Advertisers can even create their  
 10 own tracking parameters by building a “custom event.”<sup>19</sup>

11 28. One such Business Tool is the Facebook Tracking Pixel. Facebook offers this piece  
 12 of code to advertisers, like BlueChew, to integrate into their website. As the name implies, the  
 13 Facebook Tracking Pixel “tracks the people and type of actions they take.”<sup>20</sup> When a user accesses  
 14 a website hosting the Facebook Tracking Pixel, Facebook’s software script surreptitiously directs  
 15 the user’s browser to contemporaneously send a separate message to Facebook’s servers. This  
 16 second secret and contemporaneous transmission contains the original GET request sent to the host  
 17 website, along with additional data that the Facebook Tracking Pixel is configured to collect. This  
 18 transmission is initiated by Facebook code and concurrent with the communications with the host  
 19 website. At relevant times, two sets of code were thus automatically run as part of the browser’s

20 <sup>16</sup> FACEBOOK, THE META BUSINESS TOOLS, <https://www.facebook.com/help/331509497253087>.

21 <sup>17</sup> See FACEBOOK, META FOR DEVELOPERS: META PIXEL, ADVANCED,  
 22 <https://developers.facebook.com/docs/meta-pixel/advanced/>; see also FACEBOOK, BEST PRACTICES  
 23 FOR META PIXEL SETUP,  
 24 <https://www.facebook.com/business/help/218844828315224?id=1205376682832142>; FACEBOOK,  
 25 META FOR DEVELOPERS: MARKETING API - APP EVENTS API,  
 26 <https://developers.facebook.com/docs/marketing-api/app-event-api/>.

27 <sup>18</sup> FACEBOOK, SPECIFICATIONS FOR META PIXEL STANDARD EVENTS,  
 28 <https://www.facebook.com/business/help/402791146561655?id=1205376682832142>.

<sup>19</sup> FACEBOOK, ABOUT STANDARD AND CUSTOM WEBSITE EVENTS,  
<https://www.facebook.com/business/help/964258670337005?id=1205376682832142>; see also  
 FACEBOOK, META FOR DEVELOPERS: MARKETING API – APP EVENTS API,  
<https://developers.facebook.com/docs/marketing-api/app-event-api/>.

<sup>20</sup> FACEBOOK, RETARGETING, <https://www.facebook.com/business/goals/retargeting>.

1 attempt to load and read BlueChew’s Website—BlueChew’s own code and Facebook’s embedded  
2 code.

3 29. Facebook’s own documentation makes clear how extensively the Facebook  
4 Tracking Pixel tracks private information. It describes the Facebook Tracking Pixel as code that  
5 Facebook’s business customers can put on their website to “[m]ake sure your ads are shown to the  
6 right people[] [and] *find . . . people who have visited a specific page or taken a desired action on*  
7 *your website*” (emphasis added).<sup>21</sup>

8 30. Facebook instructs such business customers that:

9 Once you’ve set up the [Facebook Tracking] Pixel, *the pixel will log when someone*  
10 *takes an action on your website*. Examples of actions include adding an item to their  
11 shopping cart or making a purchase. *The Pixel receives these actions, or events,*  
12 *which you can view on your [Facebook Tracking] Pixel page in Events Manager.*  
13 *From there, you’ll be able to see the actions that your customers take. You’ll also*  
14 *have options to reach those customers again through future Meta ads.*<sup>22</sup>

15 31. This tracked information includes private data revealing prescribed medications  
16 purchased by patients on the BlueChew Website.

17 32. The Facebook Tracking Pixel code enables Facebook not only to help BlueChew  
18 with advertising to its own patients outside the Website, but also includes individual patients  
19 among groups targeted by *other* Facebook advertisers relating to the conditions about which  
20 patients communicated on BlueChew’s Website.

21 33. Facebook’s Business Help Center explains:

22 Meta *uses event data to show ads to people who are likely to be interested in them.*  
23 One type of marketing data is website events, which are *actions that people take on*  
24 *your website*.<sup>23</sup>

25 34. In other words, Facebook sells advertising space by highlighting its ability to target

26 <sup>21</sup> META, ABOUT META PIXEL,  
27 <https://www.facebook.com/business/help/742478679120153?id=1205376682832142>.

28 <sup>22</sup> *Id.* (emphasis added).

<sup>23</sup> META, ABOUT STANDARD AND CUSTOM WEBSITE EVENTS,  
<https://www.facebook.com/business/help/964258670337005?id=1205376682832142> (emphasis added).

1 users.<sup>24</sup> Facebook can target users so effectively because it surveils user activity both on and off its  
2 site.<sup>25</sup> This allows Facebook to make inferences about users beyond what they explicitly disclose,  
3 like their “interests,” “behaviors,” and connections.<sup>26</sup>

4 35. An example illustrates how the Facebook Tracking Pixel works. Take an individual  
5 who, at relevant times, navigated to BlueChew’s Website and clicked on a link to purchase  
6 prescription medication. When that link was clicked, the individual’s browser sent a GET request  
7 to BlueChew’s server requesting the server to load the particular webpage. Then, the Facebook  
8 Tracking Pixel, Facebook’s embedded code, written in JavaScript, sent secret instructions back to  
9 the individual’s browser, without alerting the individual that this was happening. Facebook caused  
10 the browser to secretly duplicate the communication with BlueChew, transmitting it to Facebook’s  
11 servers, alongside additional information that transcribed the communication’s content and the  
12 individual’s identity.

13 36. Examples of these interceptions from the BlueChew Website are provided in  
14 Figures 5 and 6 below:  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24

---

25 <sup>24</sup> META, WHY ADVERTISE ON FACEBOOK, INSTAGRAM AND OTHER META TECHNOLOGIES,  
26 <https://www.facebook.com/business/help/205029060038706> (last visited May 21, 2024).

27 <sup>25</sup> META, ABOUT META PIXEL,  
28 <https://www.facebook.com/business/help/742478679120153?id=1205376682832142>.

<sup>26</sup> META, AD TARGETING: HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS,  
<https://www.facebook.com/business/ads/ad-targeting>.

**Figures 5 and 6:**

```

id      3074830112604017
ev      CompleteRegistration
dl      https://app.bluechew.com/medical
rl
if      false
ts      1725047922452
cd[fn]  Jimmy
cd[ln]  Anderson
cd[db]  July 10, 2001
cd[st]  Florida
cd[em]  thommy5431@yahoo.com
sw      3072
sh      1728
udff[em] 2a9a22d88b031064ea86ff104d1cabf6b14a866c2a4adf136def1330b49fecbb
v      2.9.166
r      stable
ec      7
o      6174
fbp     fb.1.1725047569640.118057358755152954
ler     empty
cdl     API_unavailable
it      1725047569594
coo     false
eid     2dbef376-e9f9-4d60-aa6f-57e6cc7f8680
rqm     GET

```

```

id      3074830112604017
ev      AddToCart
dl      https://app.bluechew.com/plans
rl
if      false
ts      1725047590601
cd[content_id] 1
sw      3072
sh      1728
v      2.9.166
r      stable
ec      1
o      4126
fbp     fb.1.1725047569640.118057358755152954
ler     empty
cdl     API_unavailable
it      1725047569594
coo     false
eid     4e93e818-65da-46db-8289-afa239434f77
rqm     GET

```

1           37. Through the Facebook Tracking Pixel, Defendant Facebook intercepted and  
2 recorded “AddToCart” and “CompleteRegistration” events, which detail information about which  
3 prescription the patient was purchasing on the Website.

4           38. As shown in Figure 5, Facebook intercepts patients’ PII, including first and last  
5 name, date of birth, and email address when they are completing the BlueChew medical profile.

6           39. As shown in Figure 6, Facebook intercepts information related to patients’  
7 prescription medications.

8           40. Each of BlueChew’s medications are assigned their own unique content ID. These  
9 unique IDs indicate the type of medication being purchased by patients, as well as the quantity and  
10 dosage. For example, the content ID “1” indicates that a patient has selected a 6-pack of  
11 BlueChew’s 30 mg Sildenafil prescription medication. Similar unique IDs are used for all varieties  
12 of BlueChew’s prescriptions. Based on these unique IDs, Facebook can readily determine  
13 information about the prescription medication being purchased by BlueChew’s patients.

14           41. Each time Facebook intercepted this activity data through the Facebook Tracking  
15 Pixel, it also disclosed a patient’s personally identifiable information, including their Facebook ID  
16 (“FID”). An FID is a unique and persistent identifier that Facebook assigns to each user. With it,  
17 any ordinary person can look up the user’s Facebook profile and name. Notably, while Facebook  
18 can easily identify any individual on its Facebook platform with only their unique FID, so too can  
19 any ordinary person who comes into possession of an FID. Facebook admits as much on its  
20 website. Indeed, ordinary persons who come into possession of the FID can connect to any  
21 Facebook profile.

22           42. A user who accessed the Website while logged into Facebook transmitted what is  
23 known as a “c\_user cookie” to Facebook, which contains that user’s unencrypted FID.

24           43. When a visitor’s browser had recently logged out of an account, Facebook  
25 compelled the visitor’s browser to send a smaller set of cookies.

26           44. One such cookie was the “fr cookie” which contained, at least, an encrypted FID  
27  
28

1 and browser identifier.<sup>27</sup> Facebook, at a minimum, used the fr cookie to identify users.<sup>28</sup>

2 45. If a visitor had never created an account, an even smaller set of cookies was  
3 transmitted.

4 46. At each stage, the Website also utilized the “\_fbp cookie,” which attached to a  
5 browser as a first-party cookie, and which Facebook used to identify a browser and a user.<sup>29</sup>

6 47. The c\_user cookie expires after 90 days if the user checked the “keep me logged in”  
7 checkbox on the website.<sup>30</sup> Otherwise, the c\_user cookie is cleared when the browser exits.<sup>31</sup>

8 48. The fr cookie expires after 90 days unless the visitor’s browser logs back into  
9 Facebook.<sup>32</sup> If that happens, the time resets, and another 90 days begins to accrue.<sup>33</sup>

10 49. The \_fbp cookie expires after 90 days unless the visitor’s browser accesses the same  
11 website.<sup>34</sup> If that happens, the time resets, and another 90 days begins to accrue.<sup>35</sup>

12 50. The Facebook Tracking Pixel used both first- and third-party cookies. A first-party  
13 cookie is “created by the website the user is visiting”—*i.e.*, the Website.<sup>36</sup> A third-party cookie is  
14 “created by a website with a domain name other than the one the user is currently visiting”—*i.e.*,  
15 Facebook.<sup>37</sup> The \_fbp cookie was always transmitted as a first-party cookie. A duplicate \_fbp  
16

---

17 <sup>27</sup> DATA PROTECTION COMMISSIONER, FACEBOOK IRELAND LTD, REPORT OF RE-AUDIT (Sept. 21,  
18 2012), [http://www.europe-v-facebook.org/ODPC\\_Review.pdf](http://www.europe-v-facebook.org/ODPC_Review.pdf).

19 <sup>28</sup> FACEBOOK, PRIVACY CENTER – COOKIES POLICY,  
20 <https://www.facebook.com/privacy/policies/cookies/?subpage=subpage-1.3>.

21 <sup>29</sup> *Id.*

22 <sup>30</sup> Seralthan, FACEBOOK COOKIES ANALYSIS (Mar. 14, 2019),  
23 <https://techexpertise.medium.com/facebook-cookies-analysis-e1cf6ffbf8a>.

24 <sup>31</sup> *Id.*

25 <sup>32</sup> *See id.*

26 <sup>33</sup> Confirmable through developer tools.

27 <sup>34</sup> FACEBOOK, PRIVACY CENTER – COOKIES POLICY,  
28 <https://mbasic.facebook.com/privacy/policies/cookies/printable/#annotation-1>.

<sup>35</sup> Also confirmable through developer tools.

<sup>36</sup> PC MAG, FIRST-PARTY COOKIE, <https://www.pcmag.com/encyclopedia/term/first-party-cookie>.  
This is confirmable by using developer tools to inspect a website’s cookies and track network activity.

<sup>37</sup> PC MAG, THIRD-PARTY COOKIE, <https://www.pcmag.com/encyclopedia/term/third-party-cookie>.  
This is also confirmable by tracking network activity.

1 cookie was sometimes sent as a third-party cookie, depending on whether the browser had recently  
2 logged into Facebook.

3 51. Facebook, at a minimum, used the fr, \_fbp, and c\_user cookies to link to FIDs and  
4 corresponding Facebook profiles. Facebook intercepted these identifiers alongside the event data.

5 52. Alternatively, Facebook can also match this prescription information to the specific  
6 BlueChew patient based on the PII intercepted from the patient's medical profile.

7 53. After collecting and intercepting the information described in the preceding  
8 paragraphs, Facebook processed, analyzed, and assimilated it into datasets like Core Audiences and  
9 Custom Audiences.

10 54. Plaintiff never consented, agreed, authorized, or otherwise permitted Facebook to  
11 disclose his PII and PHI.

### 12 **C. Google's Tracking Technology on the BlueChew Website**

13 55. Google is one of the most valuable publicly traded companies in the world with a  
14 market capitalization of over \$1 trillion dollars. Google fancies itself a "tech" company, but  
15 Google, at its core, is an advertising company.

16 56. Google "make[s] money" from "advertising products [that] deliver relevant ads at  
17 just the right time," generating "revenues primarily by delivering both performance advertising and  
18 brand advertising."<sup>38</sup> In 2020, Google generated \$146.9 billion in advertising revenue, which  
19 amounted to more than 80 percent of Google's total revenues for the year. Google generated an  
20 even higher percentage of its total revenues from advertising in prior years:

21 **Figure 7:**

22 Year	Total Revenue	Ad Revenue	% Ad Revenue
23 2021	\$257.6 billion	\$209.5	81.33%
24 2020	\$182.5 billion	\$146.9 billion	80.49%
25 2019	\$161.9 billion	\$134.8 billion	83.29%
26 2018	\$136.8 billion	\$116.5 billion	85.12%

27 <sup>38</sup> ALPHABET INC., ANNUAL REPORT (FORM 10-K) (Feb. 2, 2021), available at  
28 <https://www.sec.gov/Archives/edgar/data/1652044/000165204421000010/goog-20201231.htm>.

1           57. Google offers several analytics products, including SDKs and a tracking pixel,  
2 which exist solely to help drive ad revenue. For instance, Google’s SDK and pixel integrate with  
3 Google’s advertising offerings, such as Google Ads, Search Ads 360, Google Cloud, and Google  
4 Ad Manager, to direct more individuals to use Google’s ad network and products increasing  
5 Google’s overall ad revenue. Products like Google’s SDK and its tracking pixel also improve the  
6 company’s advertising network and capabilities by providing more wholesome profiles and data  
7 points on individuals.

8           58. One of these SDKs and tracking pixels is Google Analytics. Google first launched a  
9 version of Google Analytics in 2005 as a tool for website traffic analysis. In 2007, Google  
10 launched Google Analytics Synchronous code with new tracking functionality, such as the ability  
11 to track commerce transactions. Two years later, Google launched the Google Analytics  
12 Asynchronous code, which allowed webpages to load faster and improved data collection and  
13 accuracy.

14           59. Google continued updating its analytics platform, launching Universal Analytics in  
15 2012. Universal Analytics offered new tracking codes and tools that provided more in-depth  
16 information about user behavior. Also, Universal Analytics enabled tracking the same user across  
17 multiple devices through its addition of the User-ID feature, which “associate[s] a persistent ID for  
18 a single user with that user’s engagement data from one or more sessions initiated from one or  
19 more devices.”

20           60. In 2020, Google launched Google Analytics 4, a platform combining Google  
21 Analytics with Firebase to analyze both app and web activity.

22           61. Since launching Google Analytics, Google has become one of the most popular web  
23 analytics platforms on the internet. Indeed, Google had a \$62.6 billion increase in advertising  
24 revenues in 2021, compared to 2020, after launching its most recent version of Google Analytics.

25           62. Google touts Google Analytics as a marketing platform that offers “a complete  
26 understanding of your customers across devices and platforms.”<sup>39</sup> It allows companies and

27 <sup>39</sup> *Analytics*, GOOGLE, <https://marketingplatform.google.com/about/analytics/> (last visited Jan. 10,  
28 2023).

advertisers that utilize it to “understand how your customers interact across your sites and apps, throughout their entire lifestyle,” “uncover new insights and anticipate future customer actions with Google’s machine learning to get more value out of your data,” “take action to optimize marketing performance with integrations across Google’s advertising and publisher tools,” and “quickly analyze your data and collaborate with an easy-to-use interface and shareable reports.”<sup>40</sup>

63. Google Analytics is incorporated into third-party websites and apps, including the Website, by adding a small piece of JavaScript measurement code to each page on the site. This code immediately intercepts a user’s interaction with the webpage every time the user visits it, including what pages they visit and what they click on. The code is also capable of collecting PII, as shown in Figures 8 and 9 below.

**Figures 8 and 9:**

sid	1725047568
sct	1
seg	1
dl	https://app.bluechew.com/medical
dr	https://app.bluechew.com/register
dt	Medical   BlueChew®
en	CompleteRegistration
_c	1
_ee	1
ep.first_name	Jimmy
ep.last_name	Anderson
ep.state	Florida
ep.email	thommy5431@yahoo.com
ep.dob	July 10, 2001
ep.event_id	2dbef376-e9f9-4d60-aa6f-57e6cc7f8680
ep.click_id	
ep.uuid_c1	

<sup>40</sup> *Id.*

sid	1725047568
sct	1
seg	1
dl	https://app.bluechew.com/plans
dt	BlueChew® Plans   Choose Sildenafil, Tadalafil, or Vardenafil
en	add_to_cart
_ee	1
pr1	id1
epn.product_id	1
ep.event_id	4e93e818-65da-46db-8289-afa239434f77
ep.click_id	
ep.uuid_c1	

64. As shown in Figure 8, Google is intercepting patients' PII, including first and last name, date of birth, and email address when they are completing the BlueChew medical profile.

65. As shown in Figure 9, Google is intercepting information related to patients' prescription medications.

66. As discussed, *supra*, each of BlueChew's medications are provided their own unique product ID. These unique IDs will indicate not only the type of medication being purchased by patients, but also the quantity and dosage. The product ID "1" indicates that a patient has selected a 6-pack of BlueChew's 30 mg Sildenafil prescription medication.

67. Once Google's software code collects the data, it packages the information and sends it to Google Analytics for processing. Google Analytics also allows the company or advertiser to customize the processing of the data, such as applying filters. Once the data is processed, it is stored on a Google Analytics database and cannot be changed.

68. After the data has been processed and stored in the database, Google uses this data to generate reports to help analyze the data from the webpages. These include reports on acquisition (e.g., information about where your traffic originates, the methods by which users arrive at your site or app, and the marketing efforts you use to drive traffic), engagement (e.g., measure user engagement by the events and conversion events that users trigger and the web pages and app screens that user visits, and demographics (e.g., classify your users by age, location, language, and gender, along with interests they express through their online browsing and purchase activities).

69. In addition to using the data collected through Google Analytics to provide marketing and analytics services, Google also uses the data collected through Google Analytics to improve its ad targeting capabilities and data points on users.

70. Google Analytics can also be linked with Google Ads, allowing the data intercepted by Google Analytics to be utilized for targeted advertising purposes.<sup>41</sup>

71. The Website utilizes Google's pixel and SDK. As a result, Google intercepted patients' interactions on the Website, including their PII and PHI. Google received at least "Custom Events" and URLs that disclosed the name of the prescription medication and the medication quantity and dosage. Google also received additional PII, including first and last name, email address, and date of birth, that uniquely identify the patient, as shown below in Figures 8 and 9.

72. Plaintiff and Class Members provided their PII, PHI, and other sensitive data to BlueChew to obtain medical prescriptions. This information was intercepted by Google without Plaintiff's consent or knowledge.

73. By law, Plaintiff is entitled to privacy in his protected health information and confidential communications. Defendants deprived Plaintiff of his privacy rights when they: (1) implemented a system that surreptitiously tracked, recorded, and disclosed Plaintiff's and other online patients' confidential communications, personally identifiable information, and protected health information; (2) disclosed and/or intercepted patients' protected health information; and (3) undertook this pattern of conduct without notifying Plaintiff and without obtaining his express written consent.

#### **CLASS ACTION ALLEGATIONS**

74. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23 individually and on behalf of a class defined as all natural persons in California who, during the class period, purchased medication on [www.bluechew.com](http://www.bluechew.com) (the "Class").

---

<sup>41</sup> <https://support.google.com/analytics/answer/9379420?hl=en#zippy=%2Cin-this-article>

1           75. Plaintiff reserves the right to modify the class definitions or add sub-classes as  
2 necessary prior to filing a motion for class certification.

3           76. The “Class Period” is the time period beginning on the date established by the  
4 Court’s determination of any applicable statute of limitations, after consideration of any tolling,  
5 concealment, and accrual issues, and ending on the date of entry of judgement.

6           77. Excluded from the Class are Defendants; any affiliate, parent, or subsidiary of  
7 Defendants; any entity in which Defendants have a controlling interest; any officer, director, or  
8 employee of Defendants; any successor or assign of Defendants; anyone employed by counsel in  
9 this action; any judge to whom this case is assigned, his/her spouse and immediate family  
10 members; and members of the judge’s staff.

11           78. Numerosity. Members of the Class are so numerous that joinder of all members is  
12 impracticable. The exact number of Class Members is unknown to Plaintiff at this time. However,  
13 it is estimated that there are at least thousands of individuals in the Class. The identity of such  
14 membership is readily ascertainable from Defendants’ records.

15           79. Typicality. Plaintiff’s claims are typical of the claims of the Class because Plaintiff  
16 used www.bluechew.com to purchase a prescription for erectile dysfunction medication and had  
17 his personally identifiable information and protected health information disclosed to Facebook and  
18 Google without his express written authorization or knowledge. Plaintiff’s claims are based on the  
19 same legal theories as the claims of other Class Members.

20           80. Adequacy. Plaintiff is prepared to take all necessary steps to represent fairly and  
21 adequately the interests of the Class Members. Plaintiff’s interests are coincident with, and not  
22 antagonistic to, those of the members of the Class. Plaintiff is represented by attorneys with  
23 experience in the prosecution of class action litigation, generally, and in the emerging field of  
24 digital privacy litigation, specifically. Plaintiff’s attorneys are committed to vigorously  
25 prosecuting this action on behalf of the members of the Class.

26           81. Commonality. Questions of law and fact common to the members of the Class  
27 predominate over questions that may affect only individual members of the Class because  
28 Defendants have acted on grounds generally applicable to the Class. Such generally applicable

conduct is inherent in Defendants' wrongful conduct. Questions of law and fact common to the Class include:

- a. Whether Defendants intentionally tapped the lines of internet communication between patients and their healthcare provider;
- b. Whether Defendants' software code surreptitiously recorded personally identifiable information, protected health information, and related communications;
- c. Whether Facebook and Google are third-party eavesdroppers;
- d. Whether Defendants' disclosures of personally identifiable information, protected health information, and related communications constituted an affirmative act of communication;
- e. Whether Defendants violated Plaintiff's and Class Members' privacy rights by using their software code to record and communicate patients' confidential medical communications;
- f. Whether Plaintiff and Class Members are entitled to damages under CIPA or any other relevant statute; and
- g. Whether Defendants' actions violated Plaintiff's and Class Members' privacy rights as provided by the California Constitution.

60. Superiority. Class action treatment is the superior method for the fair and efficient adjudication of this controversy. Such treatment permits a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, or expense that numerous individual actions would engender. The benefits of proceeding through the class mechanism, including providing injured persons or entities a method for obtaining redress on claims that could not practicably be pursued individually, substantially outweigh any potential difficulties in the management of this class action. Plaintiff knows of no special difficulty to be encountered in litigating this action that would preclude its maintenance as a class action.

**COUNT I**  
**Violation of the California Invasion of Privacy Act,**  
**Cal. Penal Code § 631**

82. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein and brings this count individually and on behalf of the members of the Class against Defendants.

83. The California Invasion of Privacy Act (the “CIPA”) is codified at California Penal Code Sections 630 to 638. The CIPA begins with its statement of purpose—namely, that the purpose of the CIPA is to “protect the right of privacy of the people of [California]” from the threat posed by “advances in science and technology [that] have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications . . .” Cal. Penal Code § 630.

84. A person violates California Penal Code Section 631(a), if:

by means of any machine, instrument, or contrivance, or in any other manner, [s/he] intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or [s/he] willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or [s/he] uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained . . .<sup>42</sup>

85. To avoid liability under section 631(a), a defendant must show it had the consent of all parties to a communication.

86. At all relevant times, Defendants tracked and intercepted Plaintiff’s and Class Members’ internet communications while using www.bluechew.com to buy prescription medications. These communications were intercepted without the authorization and consent of Plaintiff and Class Members.

---

<sup>42</sup> Cal. Penal Code § 631(a).

1           87. Defendants intended to learn some meaning of the content in the URLs and the  
2 content the visitors requested.

3           88. The following items constitute “machine[s], instrument[s], or contrivance[s]” under  
4 the CIPA, and even if they do not, Defendants’ SDKs and other software code fall under the broad  
5 catch-all category of “any other manner”:

- 6           a. The computer codes and programs Facebook and Google used to track Plaintiff and  
7 Class Members’ communications while they were navigating www.bluechew.com;
- 8           b. Plaintiff’s and Class Members’ browsers;
- 9           c. Plaintiff’s and Class Members’ computing and mobile devices;
- 10          d. Defendants’ web and ad servers;
- 11          e. The web and ad servers from which Facebook and Google tracked and intercepted  
12 Plaintiff’s and Class Members’ communications while they were using a web  
13 browser to access or navigate www.bluechew.com;
- 14          f. The computer codes and programs used by Facebook and Google to effectuate their  
15 tracking and interception of Plaintiff’s and Class Members’ communications while  
16 they were using a browser to visit www.bluechew.com; and
- 17          g. The plan Defendants’ carried out to effectuate its tracking and interception of  
18 Plaintiff’s and Class Members’ communications while they were using a web  
19 browser or mobile device to visit www.bluechew.com.

20           89. At all relevant times, Defendants, through their SDKs and other software code,  
21 intentionally tapped or made unauthorized connections with, the lines of internet communications  
22 between Plaintiff and Class Members and the Website without the consent of all parties to the  
23 communication.

24           90. Defendants, willfully and without the consent of Plaintiff and Class Members, read  
25 or attempted to read, or learn the contents or meaning of Plaintiff’s and Class Members’  
26 communications to BlueChew while the communications are in transit or passing over any wire,  
27 line or able, or were being received at any place within California when it intercepted Plaintiff’s  
28 and Class Members’ communications and data with BlueChew.

1           91. Defendants used or attempted to use the communications and information they  
2 received through their tracking technology, including to supply advertising services.

3           92. The information intercepted by Defendants, such as information related to  
4 prescription medications, constituted protected health information.

5           93. As a result of the above violations, Defendants are liable to Plaintiff and other Class  
6 Members in the amount of \$5,000 dollars per violation or three times the amount of actual  
7 damages, whichever is greater. Additionally, California Penal Code Section 637.2 specifically  
8 states that “[it] is not a necessary prerequisite to an action pursuant to this section that the plaintiff  
9 has suffered, or be threatened with, actual damages.”

10           94. Under the CIPA, Defendants are also liable for reasonable attorney’s fees, and other  
11 litigation costs, injunctive and declaratory relief, and punitive damages in an amount to be  
12 determined by a jury, but sufficient to prevent the same or similar conduct by Defendants in the  
13 future.

14                               **COUNT II**  
15                               **Violation of the California Invasion of Privacy Act,**  
16                               **Cal. Penal Code § 632**

17           95. Plaintiff repeats the allegations contained in the paragraphs above as if fully set  
18 forth herein and brings this count individually and on behalf of the members of the Class against  
19 Defendants.

20           96. Cal. Penal Code § 632 prohibits “intentionally and without the consent of all parties  
21 to a confidential communication,” the “use[] [of] an electronic amplifying or recording device to  
22 eavesdrop upon or record the confidential communication.”

23           97. Section 632 defines “confidential communication” as “any communication carried  
24 on in circumstances as may reasonably indicate that any party to the communication desires it to be  
25 confined to the parties thereto[.]”

26           98. Plaintiff’s and Class Members’ communications to BlueChew, including their  
27 sensitive personal and health information, such as information related to their prescription  
28 medications, were confidential communications for purposes of § 632, because Plaintiff and Class  
Members had an objectively reasonable expectation of privacy in this data.



1 Defendants.

2 107. Plaintiff and Class Members have an interest in: (1) precluding the dissemination  
3 and/or misuse of their sensitive, confidential communications and protected health information;  
4 and (2) making personal decisions and/or conducting personal activities without observation,  
5 intrusion, or interference, including, but not limited to, the right to visit and interact with various  
6 internet sites without being subjected to wiretaps without Plaintiff's and Class Members'  
7 knowledge or consent.

8 108. At all relevant times, by using the SDKs and other software codes to record and  
9 communicate patients' personal identifiers alongside their confidential medical communications,  
10 Defendants intentionally invaded Plaintiff's and Class Members' privacy rights under the  
11 California Constitution.

12 109. Plaintiff and Class Members had a reasonable expectation that their  
13 communications, identities, health information, and other data would remain confidential, and that  
14 Defendants would not install wiretaps on www.bluechew.com.

15 110. Plaintiff and Class Members did not authorize Defendants to record and transmit  
16 Plaintiff's and Class Members' private medical communications alongside their personally  
17 identifiable and health information.

18 111. This invasion of privacy was serious in nature, scope, and impact because it related  
19 to patients' private medical communications. Moreover, it constituted an egregious breach of the  
20 societal norms underlying the privacy right.

21 112. Accordingly, Plaintiff and Class Members seek all relief available for invasion of  
22 privacy under the California Constitution.

### 23 **PRAYER FOR RELIEF**

24 WHEREFORE, Plaintiff prays for relief and judgment, as follows:

- 25 a. For a determination that this action is a proper class action;
- 26 b. For an order certifying the Class, naming Plaintiff as representative of the
- 27 Class, and naming Plaintiff's attorneys as Class Counsel to represent the
- 28 Class;

- c. For an order declaring that Defendants' conduct violated the statutes referenced herein;
- d. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;
- e. For an award of compensatory damages, including statutory damages where available, to Plaintiff and the Class Members against Defendants for all damages sustained as a result of Defendants' wrongdoing, in an amount to be proven at trial;
- f. For punitive damages, as warranted, in an amount to be determined at trial;
- g. For an order requiring Defendants to disgorge revenues and profits wrongfully obtained;
- h. For prejudgment interest on all amounts awarded;
- i. For injunctive relief as pleaded or as the Court may deem proper;
- j. For an order awarding Plaintiff and the Class their reasonable attorneys' fees and expenses and costs of suit; and
- k. For an order granting Plaintiff and Class Members such further relief as the Court deems appropriate.

**DEMAND FOR JURY TRIAL**

Plaintiff, on behalf of himself and the proposed Class, demands a trial by jury for all of the claims asserted in this Complaint so triable.

Dated: September 10, 2024

Respectfully submitted,

**BURSOR & FISHER, P.A.**

By: /s/ L. Timothy Fisher  
L. Timothy Fisher

L. Timothy Fisher (State Bar No. 191626)  
1990 North California Blvd., Suite 940  
Walnut Creek, CA 94596

Telephone: (925) 300-4455  
Facsimile: (925) 407-2700  
Email: ltfisher@bursor.com

*Counsel for Plaintiff*